Cyber Network Defense Team - Service Catalog

Fiscal Year 2016-2017 Service Update

Version 3.0

Updated on: 9/7/2016

Service	Description	Category / Notes	Rates
Independent Security Assessment (ISA)	This biennial assessment is required by Government Code Section 11549.3 as amended by AB 670 on October 6, 2015. This phased assessment is designed to provide a wide reaching analysis of the current state of the logical cybersecurity controls within the assessed entity. Assessment areas within this phase include asset inventory, vulnerability scanning, phishing resistance assessment, firewall analysis, and system hardening and limited policy analysis as it related to assess control under NIST 800-53. (Notes: 1-3, 6-7)	**ISA-A (1-500)**	***$42,508.23***
		ISA-B (500-1000)	***$48,037.38***
		ISA-C (1001-2000)	***$59,527.62***
		ISA-D (2001-3000)	***$68,685.22***
		ISA-E (3001-4000)	**$77,842.82**
		ISA-F (4001-5000)	***89,333.05***
		ISA-G (5001-7500)	**$117,324.69**
		ISA-H (7501-10000)	**$150,715.55**
		ISA-J (10000-15000)	**$221,428.60**
		ISA-K (15001-20000)	**$297,540.87**
		ISA-M (20001-25000)	**$364,322.60**
		ISA-N (25001-30000)	**$431,104.32**
		ISA-X (30001 +)	***Call for Quote***
Combined Independent Security Assessment (ISA) & Hybrid Penetration Test (HPT) single Service Offering (ISAP)	This service combines the biennial ISA assessment as required by AB 670 with a Hybrid Penetration Test as a single service offering. In addition to the ISA (see ISA offering), this service includes a Hybrid, red-team oriented, penetration test. These services include both passive and active network reconnaissance, target development, probing of selected external facing web applications, attempted host implantation, data exfiltration, host pivoting attempts, and artifact collection. A detailed findings report including recommendations are provided. (Notes: 1-6)	**ISAP-1 (1-500)**	***$57,323.73***
		ISAP-2 (500-1000)	***$63,117.36***
		ISAP-3 (1001-2000)	***$75,136.56***
		ISAP-4 (2001-3000)	***$84,690.88***
		ISAP-5 (3001-4000)	**$94,245.20**
		ISAP-6 (4001-5000)	***106,264.40***
		ISAP-7 (5001-7500)	**$135,842.94**
		ISAP-8 (7501-10000)	**$170,820.69**
	Cont. Next page…	**ISAP-9 (10000-15000)**	**$245,236.49**

Service	Description	Category / Notes	Rates
ISAP Continued…		**ISAP-10 (15001-20000)**	**$325,051.51**
		ISAP-11 (20001-25000)	**$395,007.32**
		ISAP-12 (25001-30000)	**$464,962.53**
		ISA-X (30001 +)	***Call for Quote***
Phishing Susceptibility Sampling Service (PSS)	This service is a stand-alone offering designed to assist organizations evaluate the effectiveness of their anti-phishing training. Service includes the development of a organizational relevant phishing campaign and managed phishing experience. Results reporting include metrics for # users who click the phishing link and the number of users that provide network credentials resulting from the attempt. Service includes up to 1000 email addresses per campaign.	**7**	***$ 2,019.03***
Agency Vulnerability Assessment (AVA)	Perform an asset discovery scan for up to 12 Class C IP Ranges (or equiv) and subsequent credentialed vulnerability assessment for the identified system hosts properly configured and available for scanning during the assessment window. Deliverables include detailed findings reports and Recommendations. Service supports Windows, Macintosh, and Linux variants. Costs based on a scan for up to 3000 assets.	1	**$ 23,321.06**
Health Sampling Assessment (HSA)	Analysts perform a system vulnerability assessment of up to 150 systems located on the same logical network segment and generate a comprehensive findings report. This service is recommended for agencies attempting to assess the effectiveness of current organizational security patching ahead of an audit, security assessment, or as part of the independent analysis of a non-government delivered system(s).	1, 8	**$ 9,801.58**

Service	Description	Category / Notes	Rates
Firewall Configuration Assessment (FCA)	Analyst performs Firewall Analysis & Compliance Review on specified firewall / device. Analysis and analytics will address security configuration and best practices, manageability, access controls, change management compliance (rule traceability; documented change requests, etc...); identification of overlapping or redundant rules; identification of unused rules; review firewall architecture for appropriate zone implementation, segmentation, and intercommunication; access compliance with applicable state firewall compliance rules..	2	**$ 9,671.40**
Website Configuration Vulnerability Scan (WCV)	An analysis of web site and the directly subordinate pages as accessed from the root or sub-site of the specified URL (e.g. www.acme.ca.gov includes www.acme.ca.gov/service, etc...). Analysis considers risk exposure regarding information disclosure, Structured Query Language Injection (SQLi) susceptibility, resistance to Cross-Site Scripting (XXS) vulnerability. The scan will not attempt to compromise the host through vulnerability exploitation. Scanning is conducted externally and internally to identify Access Control Lists and other security differences from an "Insider Threat" perspective.	3	**$ 9,880.48**
Network Traffic Anomaly and Indicators of Compromise (NIC)	Acquisition of raw network traffic captures from client network. Traffic will be replayed against multiple Intrusion Detection System engines and traffic analysis tools to perform a best effort analysis for the presence of Indicators of Compromise (IoC). Traffic analysis results to be provided via formal report and metrics.	4	**$ 13,489.05**

Service	Description	Category / Notes	Rates
Hybrid Penetration Testing (HPT)	Hybrid Penetration Test is a red-team oriented service that includes both passive and active network reconnaissance, target development, probing of selected external facing web applications, attempted host implantation, data exfiltration, host pivoting attempts, and artifact collection. A detailed findings report including recommendations are provided. Rate is estimate based on 3,000 WAN connected endpoints. Rates billed based on total assets. Cost an estimate please contact the CND	1-2, 5	**$ 65,491.42**
System Engineering and Support (SES)	This service is designed to provide an adhoc Information Technology Engineering and Best Practice deployment support solution in direct support of a unique client requirement. Since each client requirement is unique (Scope, architecture, and requirements), this solution requires direct coordination with a CND representative to determine if an appropriate engineer is available to your the agency needs. Support is bill in Daily (8 hour) increments.		**$ 905.83**
Active Directory Health Analysis (AHA)	Perform analysis of one Active Directory Forest or Domain (as applicable to customer) to evaluate the operations of the agencies Active Directory forest infrastructure based upon a series of established metrics and Best Business Practices (BBPs) that address forest health, replication services, directory supporting services, separation of duties, and logical access control implementation. Physical access to agencies Forest Domain Controller(s) must be provided by agency.		**$ 25,821.81**

Service	Description	Category / Notes	Rates
Security Content Automation Protocol Baseline Image Analysis (BIA)	Perform analysis of logical controls related to NIST 800-53 compliance using the Security Content Automaton Protocol (SCAP) logical analysis tool for up to 10 systems less than 50 miles form CND HQ. Service includes the analysis, collection of results, correlation of results into actionable recommendations, and presentation of the report.	6	**$ 5,298.57**
Incident Response Support Services (IRS)	This service is designed to provide an agency engaged in Incident Response (IR) Operations with 2 additional support personnel for a day with the appropriate goal related skillsets (as identified by the agency & within the CND capability set) to augment ongoing, long-term recovery operations. Due to the dynamic nature of IR recovery operations, the agency may request in advance uniquely qualified team members be layer into different phases of the recovery efforts (e.g. Exchange Engineer on Days 1-2, Symantec Engineer on Days 3-5, etc...). Specialty requirements must be negotiated in advance. Service is billed at the daily rate.		**$ 2,388.31**

Notes:

All previous pricing is superseded by this updated Service Catalog. Catalog pricing represents sample costs based on commonly requested quantities. Some services costs are dependent on system or device counts which may lower or raise these sample cost projections. Actual cost is reflected on the CND issued IAA and is based on the specified statement of work.

Previously issued IAA pricing is grandfathered for 30 days from date of catalog change. IAA received after the 30 day window require reissuance to reflect the updated costs and terms.

Scan service costs are based on general Endpoint numbers and provide a +/- 5% variance. Customers are encouraged to request a custom estimate for their specific needs to ensure the best cost avoidance. Customers should review their Active Directory, Asset inventories, and Non-Windows management tool to provide as accurate as possible asset estimate

1 - Assessment conducted from a single location with LAN/WAN connectivity adequate for the assessment of the target systems. Agency must comply with pre-scan configuration requirements to ensure maximum asset access. Scans are conducted as a best effort service. Systems not configured in accordance with prescan guidance or otherwise not available for scan during the pre-agreed upon scan period will not be included in the final results.

2 - Cost applies per configuration. HA pairs are considered two firewalls. Clients should assess only the primary firewall since pairs are directly replicated. Results may be provided using NIST, PCI, ISO, NERC standards as specified in customer request.

3 - Scan scope limited to Root and logical subordinate pages (e.g. www.acme.com and acme.com/a, etc..). Scanner is configured to not crawl external site to the scanned host. Client will be required to provide user-level authentication credentials for sites with logon protections.

4 - Raw packet capture at network point of egress /ingress subject to 24 hours of total collection or a maximum total packet capture size of 1.5TB

5 - Pentests are billed based on the number of systems on the network (+/-) 5% variance. Test is designed to detect misconfigurations and other architecture flaws related to insecure IT operations. Test is limited to five days of onsite access and does not guarantee that all know and unknown risks will be identified in the time allotted. Client required to acknowledge risks associated with Penetration testing prior to engagement. Pay loaded targets will be selected from OSINT results unless otherwise specified in the Rules of Engagement.

6 - Baseline image analysis does not cover all operating systems. Please verify requires systems are supported.

7. Nominated phishing users are supplied by the organization. Population should include Executives, System Administrators, and representative populations for each business unit. Organization will provide user list in CSV format that includes the fields FirstName, LastName, and EmailAddress.

8. If the organizations total asset count exceeds 150 assets, this service will not satisfy the prior vulnerability scanning requirements of an ISA.